conferenceseries.com

World Congress on QUANTUM PHYSICS CONFERENCE

May 23-24, 2022 | Webinar

Quantum Cryptography

Padmapriya Pravinkumar
SASTRA Deemed to be University, India

At present, researchers have been proving mathematically that quantum computation part had quadratic speed up than the classical computation part. The breakthrough in quantum principle was established by various researchers like Feynman, who modeled the first quantum computer, later by Deutsch who introduced the properties of quantum mechanics to carry out all the information processing. Further, factorization and searching algorithms were proposed by Shor and Grover, respectively. Without these physicist researchers, parallelism, teleportation, Gram-Schmidt orthogonalization process and Pauli's exclusion principle would not have been existed to explore information processing in Quantum domain. Quantum information processing cannot be performed until the classical part (bits) is mapped onto equivalent quantum information (Qubits). The useful transformation ideology has been carried over effectively in conventional image formats preferably on the other types of information. Also, the high computational complexity requirement in the classical domain is overcome by quantum computation.

Quantum image processing will be the future targeted research field to carry out image processing, pattern recognition and geometric image manipulations. With the improvement in telemedicine applications, handling DICOM images in the health care system needs high security and governance. A traditional encryption scheme which operates on classical images presents more threat to confidentiality and integrity in maintaining patient's healthcare records. Hence quantum-based steganography and cryptographic schemes could lead to the influential authenticated tool in future quantum computers. The real-time computational difficulties in classical computing can be overcompensated with the help of quantum computing. Quantum computing provides parallelism, quantum states superposition and entanglement, coherence due to which quantum image processing and quantum cryptography fascinate the attention of researchers. The first phase in any quantum cryptosystem is to convert a classical image format into a quantum image. For this, several quantum image representations namely Flexible Representation of Quantum Images (FRQI), real ket, entangled, Multi-Channel Representation of quantum Image (MCRQI) and Novel Enhanced Quantum Representation (NEQR). Further, the quantum images are encrypted using the quantum gates like CNOT and SWAP gates due to its reversibility. Among them NEQR has been widely used in the quantum cryptography.

Biography

Padmapriya Pravinkumar received her B.E (ECE) from Angala Amman college of Engineering and Technology and completed her M.E Communication Systems from Jayaram college of Engineering and Technology. She is a university rank holder in her M.E Communication systems. She has received her Ph.D. in Wireless security from SASTRA in the year 2016. Currently, she is working as an Associate Professor in the department of ECE, SASTRA University. She has a teaching experience of 19 years and has published more than 80+ Research articles in National, International journals and in conferences and has authored 6 book chapters. She is currently guiding two doctoral students in the area of quantum cryptography. Her area of interest includes Information security, IoT, Block chain and Quantum Cryptography. She is currently working in an IoT based funded project sanctioned by SERB, INDIA. She is an incubatee in FIRST TBI, SASTRA in developing and modeling an unmanned ROBO for social cause.